ISSN 2424-5631 (online)

CYBERATTACKS AS "ARMED ATTACKS" ON THE OBJECTS OF CRITICAL INFRASTRUCTURE IN LIGHT ARTICLE 5 OF NATO TREATY

Sergii Karasov

Mykolas Romeris University, Lithuania
sergiikarasov@gmail.com

Abstract

In recent years, cyber security has become one of the most actively discussed topics of international law, not only because domestic and inter-State cyber security incidents have grown in number and severity, but also because of the realisation that the technical peculiarities of cyberspace create new and unique legal problems that previously have not been encountered.[1]

In the Wales Summit Declaration on 5 September 2014, NATO recognized that international law, including international humanitarian law and the United Nations Charter (UN Charter), applies in cyberspace. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council (NAC) on a case-by-case basis.[2]

Collective self-defense expressed in Article 5 of NATO Treaty is a well-known fundamental principle of NATO: *"…an armed attack against one or more of them in Europe or North America shall be considered an attack against them all (…)".*[3]

Although Article 5 of the NATO Treaty has no concept of the objects of armed attacks, cyberattacks as "Armed Attacks" can be carried out on Critical Infrastrucutre (CI), and on Critical Information Infrastructure (CII). Such objects can function for both military and civilian purposes. CI for civil purposes can be both in state and private

---

[1] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 621

[2] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

[3] The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

ISSN 2424-5631 (online)

ownership. The types of activities of such objects are important for the exercise of state functions.

Purpose - The present article aims at analyzing concept, types, functions of critical infrastructure and cases of cyberattacks on such objects and to determine the relationship with definition of Armed Attack in light Article 5 of the NATO Treaty.

Design/methodology/approach – the author of the article is comparing legal definitions of CI in-laws of member states of NATO that connects to cyberattacks and come across with differences and common points. The case of Estonia (cyberattack on government networks), Estonia (cyberattack on CEI) and *Stuxnet* (cyberattacks against CI) are shortly reviewed.

Findings - when it comes to cyberattacks, in most cases, it is conducted on a CII, which is directly connected and is the source of automatic control of critical infrastructure. To date, the most successful such definition is in the strategy for cybersecurity of Lithuania as a NATO member, and a partner of NATO, Finland. Case in Ukraine showed that CI works in disconnected access to the Internet network. However, working personnel periodically violated the rules of automated control and connected the Supervisory Control and Data Acquisition (SCADA)[1] to the Internet.

Research limitations/implications – the author uses NATO Treaty, legislation of the member countries of NATO to compare it and three cases of cyberattacks on CI.

Practical implications – the article could be considered by NATO' headquarters (NATO HQ), North Atlantic Council (NAC), Allied Command Transformation (ACT), NATO Communications and Information Agency (NCI Agency), NATO accredited Centres of Excellence, in particularly NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), military legal advisers to the command of NATO allies and partner countries.

Originality/Value – the problem of application of Article 5 of NATO Treaty to cyberattacks is quite new for NATO and partner countries as well. That also causes a novelty of that article – finding that cyberattacks on CI could be invoked right on the collective self-defense for NATO.

Keywords – Cyberattack, Armed Attack, NATO, Critical Infrastructure, Critical Information Infrastructure, Collective Self-Defense

Research type – research paper.

[1] Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control features in the industrial sector and energy transit infrastructure. The security of the SCADA system consists of four major elements: real-time monitoring, detection of anomalies, impact analysis and mitigation strategies.
Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4), 561. http://dx.doi.org/10.9770/jesi.2017.4.4(12)